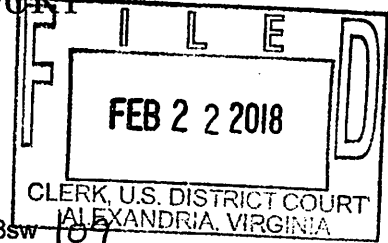


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



Case No. 1:18sw-107

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information Associated with Accounts
at Facebook, Inc., 1601 Willow Road, Menlo Park,
California

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
information associated with accounts 100010376352688 and 100011775390674, stored at the premises of Facebook, Inc., with offices at 1601 Willow Road, in Menlo Park, CA

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

Evidence of a crime contained in records associated with the social media accounts listed above, as further described in Attachment A. This warrant is sought also pursuant to 18 U.S.C. § 2703(c)(1)(A).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 2339B
18 U.S.C. § 2252

Offense Description
attempting to provide material support to terrorists
possession of child pornography

The application is based on these facts:
See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Nicholas Caslen, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/22/2018

City and state: Alexandria, VA

/s/
Michael S. Nachmanoff
United States Magistrate Judge

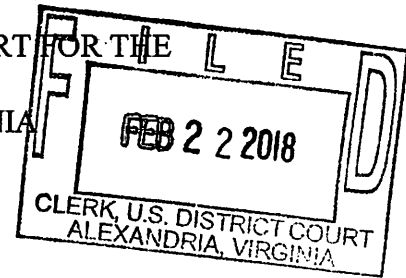
Judge's signature

Michael S. Nachmanoff, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF)
INFORMATION TO BE PROVIDED)
BY FACEBOOK, INC.)

No. 1:18sw 169

AFFIDAVIT

I, Nicholas Caslen, after being duly sworn, depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), assigned to the Washington Field Office, Joint Terrorism Task Force ("JTTF"). I have been an FBI Special Agent since 2011, and worked on the JTTF in both Wichita, Kansas, and Washington, D.C. As part of my duties, I investigate potential criminal and terrorism-related activities associated with suspected Homegrown Violent Extremists. I have participated in numerous counterterrorism investigations, during the course of which I have conducted physical surveillance, executed court authorized search warrants, and used other investigative techniques to secure relevant information regarding various crimes

2. This affidavit is submitted in support of a warrant to require the disclosure to the government of all information associated with the social media accounts with user ID numbers **100010376352688** and **100011775390674**, stored at premises owned, maintained, controlled, or operated by service provider Facebook, Inc., at 1601 Willow Road, Menlo Park, California. Based on the facts contained in this affidavit, there is probable cause to believe that within the information associated with these accounts are records, documents, communications, messages, and other information, more particularly described in Attachment A (and incorporated here), related to the attempt to provide material support to a designated terrorist organization, in

violation of 18 U.S.C. § 2339B, and/or the possession of child pornography, in violation of 18 U.S.C. § 2252.

3. I have personally participated in this investigation and have witnessed many of the facts and circumstances described herein. I have also received information from other law enforcement and intelligence officials related to this investigation. The statements contained in this affidavit are based on my own observations, review of documents, recordings, and reliable information provided to me by other law enforcement officials. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. When in this affidavit I refer to something occurring on a specific date, I intend to convey that the event occurred on or about that date.

Probable Cause

4. On or about October 15, 2004, the United States Secretary of State designated al-Qaeda in Iraq (“AQI”), then known as Jam ‘at al Tawhid wa’al-Jihad, as a Foreign Terrorist Organization (“FTO”) under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224. On or about May 15, 2014, the Secretary of State amended the designation of AQI as a FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224 to add the alias Islamic State of Iraq and the Levant (“ISIL”) as its primary name. The Secretary also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham (“ISIS”—which is how the FTO will be referenced herein), the Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furquan Establishment for Media Production. On

September 21, 2015, the Secretary added the following aliases to the FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

I. Duncan Possessed Evidence on Memory Chips and Thumb Drives

5. In February 2016, the FBI received information regarding Sean Andrew Duncan, (hereinafter “Duncan”), a United States citizen, who moved to Sterling, Virginia in June 2017, from Pittsburgh, Pennsylvania. One of Duncan’s relatives reported that Duncan had converted to Islam, may have been radicalized, and voiced his approval of westerners being beheaded in the Middle East. Duncan’s relative reported that Duncan and his wife planned to travel to Turkey.

6. On December 6, 2017, the FBI conducted a search of Twitter and found an account associated with the phone number 443-813-7730 (“the 7730 Phone Number”). According to an open source review of Twitter, the account was created in November 2015 and has the Twitter handle @DawlahtulIslaam. The phrase “Dawlahtul Isla[a]m” is an Arabic phrase that roughly translates to “The Islamic State.” I believe that this Twitter account was controlled by Duncan, because in November 2015, Duncan listed the 7730 Phone Number in his application for a U.S. passport.

A. Travel to Turkey

7. According to U.S. Customs and Border Protection, Duncan and his wife booked a flight to Istanbul, Turkey, departing from Washington Dulles International Airport, on February 26, 2016. The reservations reflected that Duncan and his wife were scheduled to depart Turkey for Bangladesh on March 4, 2016, and return to the United States on March 20, 2016. In fact, on February 26, 2016, Duncan and his wife departed the United States for Turkey. On February 27, 2016, they were denied entry into Turkey, and returned to the United States. Upon their return, they were interviewed by the FBI.

8. According to telephone service provider records, on March 4, 2016, Duncan changed his cell phone number from the 7730 Phone Number to a number ending in 9440 ("the 9440 Phone Number").

B. Duncan's Contact with a Foreign Detained Citizen

9. On July 25, 2017, during an interview with FBI agents, an unnamed co-conspirator (hereinafter "UCC"), who was in the custody of a foreign government for actively planning to travel to join ISIS, provided information regarding Duncan. According to UCC, Duncan was one of her U.S.-based contacts who had expressed an interest in joining ISIS, expressed an interest in conducting an attack in his homeland (the United States), and provided her instructions on how to construct homemade bombs. Duncan and UCC primarily spoke on encrypted mobile messaging applications. UCC also confirmed that she communicated with Duncan on an encrypted mobile messaging account ("MM1").

10. UCC told FBI agents she first became acquainted with Duncan on social media in January 2015 when Duncan sent her a friend request. UCC and Duncan initially communicated through social media but subsequently exchanged phone numbers and communicated on encrypted mobile messaging applications.

11. According to UCC, Duncan shared news articles with her from an ISIS news outlet known as Amaq News. During their communications in early 2015, Duncan expressed agreement with ISIS spokesman Abu Mohammad Al-Adnani's statement that Muslims should be striking their own homelands. UCC recalled that when she asked Duncan directly if he supported ISIS, he replied that he did. In addition, UCC made it clear to Duncan from the start of their relationship in the beginning of 2015 that she would not communicate with him unless he was "pro-ISIS." UCC was looking for a "Salafi or an ISIS supporter" to marry and live with in Syria.

She believed she would reap “heavenly rewards” if she married an ISIS fighter who died in battle.

12. In February 2015, UCC asked Duncan if he intended to go to Syria. Duncan told UCC that he wanted to make “hijrah” to Syria and that he wanted UCC to go with him to Syria. In order for Duncan and UCC to go to Syria together, Duncan proposed marriage to UCC. Duncan’s proposal occurred over an encrypted mobile messaging application. Duncan told UCC that after they were married, he wanted to plan their trip to Syria. Duncan wanted to come to UCC’s country to propose to UCC in person, but she said it was too soon. As a result of UCC rejecting Duncan’s offer of marriage, the two broke contact in or around March 2015.

13. UCC recalled a time before they broke contact when she was upset at work due to non-Muslim women wearing shorts that exposed their bodies. UCC told Duncan via an encrypted mobile messaging application she was upset with the way these women dressed and she wanted to do something about it. Duncan replied with a link to a website, and a message saying she could “try this.” UCC stated that the link contained pictures and instructions on how to make weapons and bombs. UCC stated the link was to an article titled, “How to build a bomb in the kitchen of your Mom” from Inspire magazine.

14. In January 2016 (a month before Duncan and his wife’s trip to Turkey), Duncan asked UCC if she still wanted to go to Syria and to be his second wife. UCC asked Duncan if his current wife would be okay with UCC coming with them to Syria. Duncan stated that his wife would have to be okay with it. UCC did not agree to go, and the two broke contact again.

15. In December 2016, Duncan, utilizing an encrypted mobile messaging account, re-initiated contact with UCC. Duncan told UCC that he had come back from Turkey, from where he and his wife had been sent back to the United States. Duncan said he thought the FBI was

monitoring him, but would not elaborate on why he was deported or why the FBI was monitoring him. Duncan said he did not want to implicate himself and that his wife could keep secrets. Duncan stated that his wife knew what to say when questioned by authorities. In July 2017, the FBI reviewed the UCC's phones and confirmed there were communications between Duncan and UCC on encrypted mobile messaging applications.

C. UCE's Interaction with Duncan

16. On August 2, 2017, the FBI identified an encrypted mobile messaging account ("MM2") with a naming convention similar to the one used by UCC to communicate with Duncan ("MM1"). A review of the profile photographs for this second encrypted mobile messaging account showed a photograph of Duncan and his father. In addition, the FBI found that MM2 was associated in the encrypted messaging application with the 9440 Phone Number.

17. On August 11, 2017, an FBI undercover employee (UCE) posing as UCC, contacted Duncan, who was using MM2. UCE told Duncan that "she" had been arrested by foreign authorities. Immediately after being told this, Duncan created secure chats and self-destruct timers to destroy the content of his messages with UCE. UCE told Duncan that "she" intended to make "hijrah." Duncan stated, "Hm, you know a fence Someone to take you, and is it safe in Iraq." Later, UCE asked Duncan if he had a contact in Syria, to which Duncan responded, "No a couple have been marytred (sic)."

18. On August 20, 2017, UCE told Duncan that "she" was in contact with an individual in Libya who was attempting to facilitate "her" travel to Libya. UCE told Duncan that the Libyan contact was asking various vetting questions prior to assisting UCE. UCE told Duncan that "her" Libyan contact was asking strange questions, such as UCE's blood type and family contact. UCE then asked Duncan if he (Duncan) and his wife were asked similar questions when

they tried to travel to Syria. Duncan stated, “they won’t ask that.” Duncan further stated, “I didnt (sic) go for that Just honeymoon.”

19. However, later in the conversation, UCE asked Duncan what to do about “her” contact in Libya. Duncan recommended that UCE “. . . lie to him.” Duncan stated he had never dealt with unnecessary vetting by “contacts” and that he had “always had referrals.” Based on my training and experience, I know that ISIS uses a referral system to recruit new members, and I interpret Duncan’s statement to mean that Duncan did not get asked questions by his contacts because he had “referrals” who could give them “tazkiyah.” Tazkiyah is a recommendation from a Jihadi Shaykh from their homeland or a Mujahid already in the land of Jihad. It is a generally given by an existing member of ISIS to show an individual is trustworthy.

D. Evidence from a Detained ISIS Supporter

20. In October 2017, a foreign government (not the one in whose custody UCC was) arrested one of its nationals ("Recruiter 1") for inciting rebellion. Recruiter 1 is an ISIS recruiter who is suspected of drawing foreign fighters from around the world to Recruiter 1’s home country using social media. Recruiter 1 was married to two jihadis with connections to ISIS, one of whom is dead and the other of whom was arrested for extremism by his home country. Recruiter 1 posted a message on an electronic messaging application soliciting local and foreign Muslims to help terrorists fight government troops in Recruiter 1’s home country.

21. On December 4, 2017, during an interview with FBI agents, Recruiter 1 said she had begun recording the names and telephone numbers of individuals who had requested to join her Telegram, Facebook, or other social media and/or communication application groups. Recruiter 1’s notes included a handwritten name appearing to be “Sean Ibn Gary Duncan,” associated with the 7730 Phone Number and the associated username MM1.

E. Duncan's Phone History Research to Conduct Attacks

22. On June 29, 2017, the Allegheny County Police Department ("ACPD") provided a partial copy of Duncan's phone to the FBI. On October 6, 2017, ACPD provided the remainder of the copy to the FBI. ACPD had obtained this copy during an investigation surrounding the recent death of Duncan's infant child (the cause of death in the autopsy was inconclusive). Duncan consented in writing to ACPD's search of his phone. The FBI's review of Duncan's imaged phone revealed hundreds of internet searches between March 2017, and June 2017, for ISIS-related materials; weapons; terrorists; body armor; surveillance; defense tactics; watchlist statuses leaked, watchlist terms, watchlist explanations. Based on my training and experience, I know the above-described searches are consistent with research into how to conduct an attack and defend oneself.

II. The Search of Duncan's Residence and Obstruction of Justice

23. On December 19, 2017, United States Magistrate Judge Theresa Carroll Buchanan authorized searches of Duncan's 2013 Honda CRV automobile, as well as his residence on Courtyard Square, in Sterling, Virginia, for evidence of attempts to provide material support to ISIS, in violation of 18 U.S.C. § 2339B, as well as false statements, in violation of 18 U.S.C. § 1001. Among the items authorized for seizure in the search were files or information (including files or information on computers or phones) involving travel or attempts to travel overseas; communications with members of foreign terrorist groups, and/or foreign or U.S.-based radicalizers or facilitators, or co-conspirators; contact lists of individuals associated with foreign terrorist groups, and/or foreign or U.S.-based radicalizers or facilitators; records of internet activity, or other information identifying support for or research related to a foreign terrorist

group; and information, programs, tools or applications that may be used for overt or clandestine/covert communications, and any associated contacts or communications history.

24. On December 29, 2017, FBI agents executed the search warrants at Duncan's residence and automobile. Upon execution of the warrant at the residence, the agents knocked on the door, identified themselves as FBI, and announced that they were there to execute a search warrant. Receiving no response, the agents knocked and announced their presence again, but received no response again. The agents then forcibly opened the door, and again identified themselves as FBI, and that they were there to execute a search warrant. The agents at the front door did not see anyone.

25. Moments before the FBI agents entered the residence through the front door, Duncan ran out the back door, barefoot, and with something clenched in his fist. FBI agents guarding the back door yelled at Duncan to stop. Before stopping, Duncan threw a plastic baggie over the heads of the agents.

26. FBI agents recovered the baggie thrown by Duncan. The baggie was a clear plastic Ziploc bag, containing a memory chip stored within a thumb drive that had been snapped into pieces, and placed in a liquid substance that produced frothy white bubbles. Upon searching Duncan, agents recovered a broken casing for a thumb drive from Duncan's pants pocket.

27. Based on my training and experience, I know that thumb drives can be plugged into computers and used to store large gigabyte amounts of electronic information, to include images and documents. Based on my training and experience, I know that criminals, including terrorists and individuals involved in other crimes such as child pornography, often use thumb drives to store evidence of their criminal activity that they do not want found on their computers.

28. In light of the circumstances, I believe that Duncan fled from the house with the baggie and the memory chip and the broken thumb drive in order to conceal those items from the FBI agents that Duncan knew were about to search his house. Further, I believe that the thumb drive was snapped in pieces because Duncan altered, destroyed, and mutilated it in order to impede and obstruct the FBI's investigation of him. Similarly, based on the circumstances, I believe that the memory chip and broken thumb drive was contained in a baggie containing a liquid substance because Duncan altered, destroyed, and mutilated it in order to impede and obstruct the FBI's investigation of him.

III. Child Pornography

29. On December 29, 2017, and again on January 1, 2018, while reviewing one of the electronic devices obtained as a result of the search warrant referenced in the complaint for evidence pertaining to violations of Title 18, United States Code, Sections 1001 and 2339B, an FBI Agent observed images of what appeared to be child pornography contained within the device. Based on my training, experience, and the facts set forth below, the FBI believes that the images constitute violations of Title 18, United States Code, Sections 2252 and 2252A.

30. One item seized was a Samsung Galaxy Note 3 smartphone ("the Samsung"). On December 29, 2017, and again on January 1, 2018, while reviewing the Samsung, an FBI Agent observed images of pre-pubescent minors that appeared to be engaged in sexually explicit conduct with adult males. The images appeared to be child pornography. An FBI Agent observed other images of pre-pubescent minors posed to expose their genitalia in a sexual manner, which also appeared to be child pornography. Several of the images appeared to be screen shots of viewed websites. The pre-pubescent minors in the photos were as young as infants, and the total number of images was in the hundreds.

31. The Samsung smartphone containing the images of suspected child pornography was, in the past, registered to the 7730 Phone Number that belonged to Duncan.

32. On January 4, 2018, United States Magistrate Judge Theresa Carroll Buchanan authorized searches of electronic devices and materials seized from Duncan's residence and automobile on December 29, 2017, for evidence of the possession of child pornography, in violation of 18 U.S.C. § 2252 and 2252A.

33. After further review of two of the electronic devices obtained as a result of the search warrant referenced in the complaint for evidence pertaining to violations of Title 18, United States Code, Sections 1001 and 2339B, an FBI agent observed images of what appeared to be bloodied, deceased children located in a conflict zone similar to Syria or Iraq. There were also hundreds of images of beheadings of adult men, ISIS fighters and propaganda videos promoting ISIS extremism.

IV. Electronic Communication Accounts Identified

34. In addition to seizing the Samsung smartphone mentioned above, the FBI also seized an iPhone from Duncan's residence on December 29, 2017.

35. A review of the iPhone revealed that it contained a MSISDN number ending in 9440, which matched Duncan's previous known phone number ending in 9440. Further review of the iPhone revealed an SMS message on January 10, 2017, between the user and other individual, during which the user of the iPhone identified themselves stating, "...this is Sean."

36. As mentioned earlier, during the course of the investigation into Duncan, the FBI learned Duncan used social media platforms and mobile messaging applications to communicate with ISIS sympathizers overseas. Duncan was in contact with at least two individuals supportive

of ISIS, both whom have been arrested by national security law enforcement agencies in their home countries.

37. Based on Duncan's use of social media and mobile messaging applications to communicate with at least two known ISIS related individuals, I believe Duncan utilized his social media, emails, and mobile messaging to engage with other ISIS members and/or prospective members. I believe that Duncan may have used those electronic accounts to express his desire to join ISIS, to communicate with ISIS recruiters, and to send bomb-making information to others.

38. In addition, because child pornography was already found on electronic media belonging to Duncan, and because perpetrators of crimes involving child pornography often possess child pornography on multiple electronic devices, I submit there is probable cause to believe that Duncan collected digital images of child pornography using various electronic accounts, and stored those images on various cloud storage accounts such as those described below.

39. Furthermore, based on my training, experience, and discussions with other agents, I know that individuals involved in criminal activity such as terrorism and possession of child pornography, utilize email providers such as Google and Yahoo, as well as social media platforms to include Facebook, Instagram, Twitter, and Snapchat to communicate with other individuals involved in similar criminal activity. I also know that social media platforms such as Tumblr have features that allow users to connect with other users, chat with other users, and share content on a user's page, which can be used to further criminal activity related to terrorism and possession of child pornography. In addition, I know based on my training and experience

that email providers such as Yahoo! offer services to individuals who use their products such as cloud storage for computer files, calendars, chat features, and even social media pages. I know that individuals involved in criminal activity, such as terrorism and possession of child pornography, tend to store files such as photographs in the cloud storage provided to them by companies such as Yahoo! I further know that internet websites such as, Apple accounts, Dropbox and Evernote provide users similar types of cloud storage. Therefore, based on my training, experience, and discussions with other agents, I know that individuals who Dropbox and Evernote could use the features provided to further criminal activity related to terrorism and possession of child pornography. For these reasons, and those detailed above, I submit that there is probable cause to believe that evidence of Duncan's attempt to support terrorism and possession of child pornography will be located in the following electronic facilities, belonging to Duncan.

A. Facebook account with User ID number 100010376352688

40. According to records provided by Facebook on or about April 4, 2016, a Facebook account in the name "Sean Duncan", with user ID number **100010376352688**, was registered using email seanandrewduncan@gmail.com, and is associated with email baahith217@gmail.com and Duncan's previous known phone number ending in 7730. The account was closed on or about March 1, 2016, after Duncan and Sadeq's trip to Turkey.

41. Due to the closure of the account, the FBI issued a Preservation Request to Facebook for this account. The request was acknowledged by Facebook who stated they would take reasonable steps to preserve the account. Based on my experience with preserved records from Facebook, I know that Facebook will preserve records and provide records for closed

accounts in response to a search warrant. Therefore, I believe that records related to this account exist within Facebook's holdings.

B. Facebook account with User ID number 100011775390674

42. Also, according to records provide by Facebook on or about May 4, 2016, a Facebook account in the name "Sean Duncan-Sadeq", with user ID number **100011775390674**, was registered using email seanandrewduncan@gmail.com, and was associated with Duncan's known phone number ending in 9440. The account was opened on March 27, 2016, several days after the aforementioned Facebook account with user ID number 100010376352688 was closed.

43. A review of this account on January 11, 2018, showed that the account had been deactivated. However, the FBI issued a Preservation Request to Facebook for this account. The request was acknowledged by Facebook who stated they would take reasonable steps to preserve the account. Based on my experience with preserved records from Facebook, I know that Facebook will preserve records and provide records for closed accounts in response to a search warrant. Therefore, I believe that records related to this account exist within Facebook's holdings.

44. Based on my training and experience, I know the following about Facebook, Inc.:

- a. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public. Facebook, Inc. is located at 1601 Willow Road, Menlo Park, California.
- b. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password

retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

- c. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.
- d. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.
- e. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.
- f. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

- g. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.
- h. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.
- i. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.
- j. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.
- k. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.
- l. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.
- m. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.
- n. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

- o. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.
- p. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.
- q. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.
- r. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.
- s. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime

(e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

45. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s “Neoprint,” IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account.

46. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time.

47. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation.

48. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

49. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Facebook, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A. Upon receipt of the information described in Section A of Attachment A, government-authorized persons will review that information to locate the items described in Section B of Attachment A.

50. I am trained and experienced in identifying communications relevant to the crimes under investigation, but personnel of Facebook, Inc. are not. I also know that the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence, but employees of Facebook, Inc. are not. It would be inappropriate and impractical, however, for federal agents to search the vast computer networks of Facebook, Inc. for the relevant account and then to analyze the contents of that account on the premises of that corporation. Further, the impact on the business of that corporation would be severe.

51. Accordingly, executing a warrant to search an account at Facebook, Inc. requires an approach similar to the standard approach for executing a warrant to search papers stored in a file cabinet. Searching the subject accounts in this case for evidence of the target crimes will require that agents cursorily inspect all information produced by Facebook, Inc. in order to

ascertain which contain evidence of that crime, just as it necessary for agents executing a warrant to search a filing cabinet to conduct a preliminary inspection of its entire contents in order to determine the documents which fall within the scope of the warrant. In addition, keyword searches alone are inadequate to identify all of the information subject to seizure, because keywords search text, but many common electronic mail, database and spreadsheet applications files (which files may have been attached to electronic mail) do not store data as searchable text.

52. In order to facilitate seizure by law enforcement of the records and information sought from Facebook, Inc. through this affidavit and application with a minimum of interference with the business activities of Facebook, Inc. and to protect the rights of the subject of the investigation, and to effectively pursue this investigation, this application seeks the issuance of a warrant that would permit employees of Facebook, Inc. to assist agents in the execution of this warrant, in accordance with the procedures described in Attachment A to the warrant, which is hereby incorporated into this affidavit.

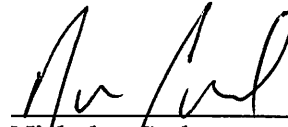
44. I am advised that, pursuant to 18 U.S.C. § 2703(a), a Court with jurisdiction over the offense that is under investigation has authority to issue a warrant to compel disclosure of stored content and records and other information pertaining to a customer or subscriber of an electronic communication service including a provider located physically in another judicial district. Accordingly, this Court has the authority to issue warrants to Facebook, Inc. for stored content and records and other information pertaining to its subscribers even though that business is located in California.

Conclusion


45. Based on the information set forth above, I submit there is probable cause to believe that the the social media accounts with user ID numbers 100010376352688 and 100011775390674, at Facebook, Inc. contains evidence of an attempt to provide material support to a designated terrorist organization, in violation of 18 U.S.C. § 2339B, and/or the possession of child pornography, violation of 18 U.S.C. § 2252, as more fully described in Attachment A.

Wherefore, I request the issuance of a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

FURTHER THIS AFFIANT SAYS NOT.


Nicholas Caslen
Special Agent, FBI

Subscribed to and sworn before me on this 22nd day of February 2018.

_____/s/ 
Michael S. Nachmanoff
~~United States Magistrate Judge~~
Michael S. Nachmanoff
United States Magistrate Judge

ATTACHMENT A (Facebook, Inc.)

A. Facebook, Inc. personnel shall isolate the information associated with Accounts **100010376352688** and **100011775390674**, and provide in electronic form to the agent who serves the search warrant an exact duplicate of that information. With respect to each account, this information includes:

- (a) All contact and personal identifying information, including passwords, security questions and answers, and screen names;
- (b) All activity logs and all other documents showing the user's posts and other Facebook activities, and all photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (c) All Photoprints and Neoprints, including profile information and all photos uploaded by that user ID or by any user that have that user tagged in them, News Feed information; status updates; links to videos; photographs, articles, and other items; Notes; Wall postings; all past and present friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (d) All records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests, as well as records of communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken; and all privacy settings and other account settings, and all records showing which Facebook users have been blocked by the account;
- (e) All "check ins" and other location information, and all IP logs, including all records of the IP addresses that logged into the account;
- (f) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked" and all information about the Facebook pages that the account is or was a "fan" of; and all records of Facebook searches performed by the account, and all information about the user's access and use of Facebook Marketplace;
- (g) All records of the length of service, the types of service utilized by the user, and the means and source of any payments associated with the service, and all cookie data and associate machines and accounts collected by Facebook for user's

account to include, but not limited to, browser information if available and other pages and groups where the user (or the associated user) is the creator.

B. Law enforcement personnel will thereafter review all information and records received from Facebook, Inc. employees to determine the information to be seized by law enforcement personnel. The information to be seized consists of information that constitutes evidence related to the attempt to provide material support to a designated terrorist organization, in violation of 18 U.S.C. § 2339B, and/or the possession of child pornography, in violation of 18 U.S.C. § 2252, including records relating to the identities of those who created, used, or communicated with the account.